

Exhibit B

UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina



FARHAD AZIMA

*Plaintiff*NICHOLAS DEL ROSSO and VITAL MANAGEMENT
SERVICES, INC.*Defendant*

Civil Action No. 20-cv-954

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS
OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Berkeley Research Group, LLC, c/o Cogency Global Inc., 122 East 42nd Street, 18th floor, New York, NY 10168

(Name of person to whom this subpoena is directed)

☒ **Production:** **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: See Attachments A and B

Place: Nelson Mullins Riley & Scarborough LLP
Attn: Lisa Herbert (We Consent to Remote Production)
330 Madison Avenue, 27th Floor, New York, NY 10017

Date and Time:

09/08/2023 5:00 pm

☐ **Inspection of Premises:** **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:

Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 08/21/2023

CLERK OF COURT

OR

*Signature of Clerk or Deputy Clerk**Attorney's signature*The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Defendants

Nicholas Del Rosso and Vital Management Services, Inc., who issues or requests this subpoena, are:
Nelson Mullins Riley & Scarborough LLP, Brandon S. Neuman, 301 Hillsborough St., Ste. 1400, Raleigh, NC 27603,
e-mail: brandon.neuman@nelsonmullins.com phone: (919) 329-3878

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 20-cv-954

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____
on *(date)* _____.

☐ I served the subpoena by delivering a copy to the named person as follows: _____

_____ on *(date)* _____; or

☐ I returned the subpoena unexecuted because: _____

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also
tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of
\$ _____.

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ 0.00 _____.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)**(c) Place of Compliance.**

(1) For a Trial, Hearing, or Deposition. A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

- (A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or
- (B) within the state where the person resides, is employed, or regularly transacts business in person, if the person
 - (i) is a party or a party's officer; or
 - (ii) is commanded to attend a trial and would not incur substantial expense.

(2) For Other Discovery. A subpoena may command:

- (A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and
- (B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) Avoiding Undue Burden or Expense; Sanctions. A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) Command to Produce Materials or Permit Inspection.

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

- (i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.
- (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) Quashing or Modifying a Subpoena.

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

- (i) fails to allow a reasonable time to comply;
- (ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);
- (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or
- (iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

- (i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

- (i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and
- (ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) Producing Documents or Electronically Stored Information. These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) Claiming Privilege or Protection.

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

- (i) expressly make the claim; and
- (ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

Attachment A

On December 18, 2020, Plaintiff Farhad Azima (“Azima”) submitted an affidavit of Christopher W. Tarbell (“Mr. Tarbell”) in the Supreme Court of Queensland, which affirmed an August 30, 2019, expert report prepared by Mr. Tarbell for Azima, attached hereto as **Attachment B** (hereinafter, the “Tarbell Report”).

The Tarbell Report, dated August 30, 2019, opines on the same data at issue in the matter at hand, *Azima v. Del Rosso and Vital Management Services, Inc.*, Case No. 20-cv-954 (M.D.N.C. filed Oct. 15, 2020). Specifically, the Tarbell Report identifies that Mr. Tarbell analyzed, *inter alia*, an “Archive of wetransfer.com file shares collected by BRG on July 13, 2018,” “Publicly available documents and websites listed in this report,” and “Data files and other materials identified below in this report.” *See Attachment B*, at ¶¶ 15(f) – (h). After analyzing this information, Mr. Tarbell opined that the WeTransfer data appears to “have been initially uploaded to WeTransfer on or about January 27, 2017.” *See Attachment B*, at ¶¶ 114–17.

It is our understanding that, during the time Mr. Tarbell authored this report, he was employed by Berkeley Research Group, LLC (“BRG”) as a Director of Cyber Security and Investigations in BRG’s New York office and that BRG archived data collected by Mr. Tarbell.

Accordingly, please produce the following documents in your possession:

1. All documents, data, and communications relied upon by Mr. Tarbell in support of the Tarbell Report, including but not limited to:
 - a. All archived data downloaded from WeTransfer that was examined by Mr. Tarbell for purposes of the Tarbell Report, specifically including the “Archive of wetransfer.com file shares collected by BRG on July 13, 2018”;
 - b. All archived data, documents, or communications evidencing or supporting Mr. Tarbell’s conclusion that “the downloadable content, distributed by WeTransfer, appears to have been at least initially uploaded to WeTransfer on or about January 27, 2017”; and
 - c. Any other “Data files and other materials” referred to or relied upon by Mr. Tarbell’s report in ¶¶ 114–17 of the Tarbell Report.

Attachment B
(Tarbell Report)

SUPREME COURT
OF QUEENSLAND

SUPREME COURT OF QUEENSLAND

REGISTRY: BRISBANE
NUMBER:

BS 13611/20

Applicant: 18 DEC 2020

FARHAD AZIMA

AND

First Respondent: DIDTHEYREADIT.COM PTY LIMITED ACN 123 027 163

AND

Second Respondent: READNOTIFY.COM PTY LTD ACN 097 291 695

COPY



ORIGINATING APPLICATION

TAKE NOTICE that the Applicant is applying to the Court for the following orders -

1. Pursuant to the Court's inherent equitable jurisdiction, the First Respondent and Second Respondent are to provide to the Applicant any documents in their possession or control that respond to the categories listed in **Annexure A**.
2. Such other orders as the Court thinks fit.
3. That the First Respondent and the Second Respondent pay the Applicant's costs of the application.

This application will be heard by the Court at

on: 20 January 2021 at 10 a.m./p.m.

Filed in the BRISBANE registry on:

18 DEC 2020

Registrar:



FEE	1020 90
INIT:	ll
REG:	BS 13611/20
ENT:	

If you wish to oppose this application or to argue that any different order should be made, you must appear before the Court in person or by your lawyer and you shall be heard. If you do not appear at the hearing the orders sought may be made without further notice to you. In addition you may before the day for hearing file a Notice of Address for Service in this Registry. The Notice should be in Form 8 to the Uniform Civil Procedure Rules. You must serve a copy of it at the applicant's address for service shown in this application as soon as possible.

APPLICATION

Filed on behalf of the Applicant
Form 5 - R.26

COOPER GRACE WARD

Level 21, 400 George Street
Brisbane 4000 Australia

T 61 7 3231 2444
F 61 7 3221 4356

ORC10236579 3465-2195-0226v1

On the hearing of the application the applicant intends to rely on the following affidavits -

1. affidavit of Oliver Robert Caine affirmed 14 December 2020;
2. affidavit of Christopher Tarbell affirmed 8 December 2020.

If you intend on the hearing to rely on any affidavits they must be filed and served at the applicant's address for service prior to the hearing date.

If you object that these proceedings have not been commenced in the correct district of the Court, you must apply to the Court for dismissal of the proceedings.

THE APPLICANT ESTIMATES THE HEARING SHOULD BE ALLOCATED -

Hours/Minutes: 90 minutes

PARTICULARS OF THE APPLICANT

Name: Farhad Azima

Applicant's residential or business address: 5921 Ward Parkway, Kansas City MO 64113

Applicant's solicitors name: Graham Roberts

Firm name: Cooper Grace Ward Lawyers

Solicitor's business address: Level 21, 400 George Street,
Brisbane QLD 4000

Address for service: c/- Cooper Grace Ward Lawyers
Level 21, 400 George Street
Brisbane QLD 4000

Telephone: (07) 3231 2404

Email: graham.roberts@cgw.com.au

Signed: 

Description: Solicitor for the Applicant

Dated: 18/12/2020

This application is to be served on: DIDTHEYREADIT.COM Pty Ltd
of 'Eugarie Commercial Centre Offices 3 & 4'
1 Eugarie Street, Noosa Heads QLD 4567

and on:

READNOTIFY.COM Pty Ltd
of 'Ascendia' Suite 3, 1 Eugarie Street
Noosa Heads QLD 4567

SUPREME COURT OF QUEENSLAND

REGISTRY: BRISBANE
NUMBER:

Applicant: **FARHAD AZIMA**

AND

First Respondent: **DIDTHEYREADIT.COM PTY LIMITED**

AND

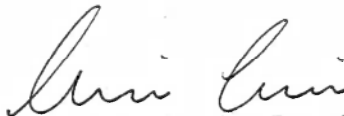
Second Respondent: **READNOTIFY.COM PTY LTD**

CERTIFICATE OF EXHIBIT

Exhibit **CC2** to the affidavit of **CHRISTOPHER TARBELL** affirmed 8 December 2020.



Deponent



~~Barrister/Solicitor/Justice of the Peace/~~

~~Commissioner for Declarations~~

CERTIFICATE OF EXHIBIT
Filed on behalf of the Applicant
Form 47 - R.435

COOPER GRACE WARD
Level 21, 400 George Street
Brisbane 4000 Australia
T 61 7 3231 2444
F 61 7 3221 4356

Expert Report of : Mr Christopher Tarbell
Specialist Field : Computer Forensics and Investigations
On behalf of : Mr Farhad Azima
Prepared for : High Court of Justice Chancery
Claim number : HC-2016-002798

Table of Contents

I.	BACKGROUND AND QUALIFICATIONS	1
II.	SCOPE OF REPORT	3
III.	ANALYSIS AND OPINIONS	5
A.	Summary	5
B.	Phishing Emails and Account Logins	9
1.	Email Accounts	9
2.	Phishing Attacks	9
3.	Phishing Emails	11
a.	October 12, 2015 Phishing Email	12
b.	October 14, 2015 Phishing Email	15
c.	October 23, 2015 Phishing Email	18
d.	November 23, 2015 Phishing Email	20
e.	November 28, 2015 Phishing Email	22
f.	MESVR	24
g.	Other Phishing Email	24
4.	Logins to fa@fal.us	25
5.	Logins to fa@farhadazima.com	26
C.	BitTorrent	29
1.	The Peer-to-Peer Network	29
2.	Azima torrent Files	31
3.	Tracking Downloads and Availability	34
D.	Data Available on the World Wide Web	35
1.	Websites and Indexing	35
2.	Data Available on Websites	36
3.	WeTransfer	39
4.	www.khater-massaad.com	40
E.	Summary of Conclusions	41
	<i>Curriculum Vitae</i> of Christopher Tarbell	44

EXPERT REPORT OF CHRISTOPHER W. TARBELL

I, Christopher W. Tarbell, provide the following expert report in connection with the above-referenced matter.

I. BACKGROUND AND QUALIFICATIONS

1. I am a computer forensics expert. I have been engaged by the solicitors acting for Mr Farhad Azima to provide an expert report to the Court in these proceedings on matters within my expertise, as set out below.

2. I understand that my duty is to help the Court and that this duty overrides any obligation to any party by whom I am engaged or who has paid or is liable to pay me. I have complied and will continue to comply with this duty. I confirm that neither my fees nor Berkeley Research Group, LLC's ("BRG") fees are dependent on the outcome of this case.

3. The facts contained in this report are true so far as they are within my own knowledge. Where I have referred to any matter that is outside my own knowledge, I have stated the source. Where I have assumed a fact to be true I have clearly stated that I have done so. I have clearly referred to the sources of any information I have used in preparing this report. The opinions I have expressed represent my true and complete professional opinions based upon my personal knowledge, education and experience. I have clearly stated any qualifications to my opinion.

4. My experience and expertise are based on the following matters. I am currently employed as a Director of Cyber Security and Investigations in BRG's New York office. BRG is a global consulting firm that is headquartered in Emeryville, California, USA. I regularly provide expert consultation to clients, including corporations, universities, and government

agencies, regarding computer and network security best-practices, as well as conduct cyber incident response and investigative analysis.

5. From 2014 to 2015, I was employed by FTI Consulting, Inc.'s Global Risk and Investigations Practice as a Managing Director of Cyber Security and Investigations, where I provided comparable services to similar clients as my current employment with BRG.

6. From 2005 to 2014, I was employed by the Federal Bureau of Investigation ("FBI") as a computer forensic examiner and Special Agent. As a member of the FBI's Computer Analysis Response Team ("CART"), my professional responsibilities focused on forensically recovering data and conducting forensic examinations of electronic evidence. As a Special Agent with the FBI, my primary professional responsibility was to conduct criminal investigations into computer and network intrusions, which also involved the retrieval and forensic examination of computer-related evidence. During the course of my career at the FBI, I worked on nearly 100 criminal and national security investigations that have involved the recovery and forensic analysis of a range of electronic evidence.

7. I earned a Master of Science degree in Computer Science from James Madison University in 2004, with a concentration in information security.

8. I have been certified as a FBI CART Forensic Examiner for both criminal and national security cases. Those certifications were in the Windows and Linux operating systems, along with mobile devices.

9. I have been certified by leading forensic software providers in the utilization of their forensic tools. For example, I have been certified by Guidance Software as an EnCase Certified Examiner and by AccessData as an AccessData Certified Examiner.

10. I have also been certified as a Forensic Computer Examiner with the International Association of Computer Investigative Specialists ("IACIS").

11. I have previously testified as a computer forensics expert. A copy of my *Curriculum Vitae* is attached to this report.

II. SCOPE OF REPORT

12. I have been instructed as an expert in the above-captioned case by the English solicitors on behalf of Defendant Mr. Farhad Azima ("Azima") to provide my analysis and opinions, based on my expertise (drawing on my education and experience), and my review of the materials described in this report, on certain matters that are in issue in these proceedings. As I understand from the pleadings filed by Azima, he contends that in around October 2015, he received emails containing malicious internet links and that they included material aimed at Azima specifically, so as to induce him to open them. He contends that by opening those links, certain persons were (unknown to him at the time) enabled to gain access to and steal Azima's confidential data (which is referred to in the pleadings as 'hacking').

13. Mr Azima's case is that beginning in around early August 2016, a substantial quantity of his private data were then placed on various websites (described as 'BitTorrent' websites). Mr Azima further says that other websites also appeared at this time, making allegations against him and providing links to the data on the 'BitTorrent' websites.

14. My report below sets out my analysis and opinions in relation to the following matters concerning these issues and allegations:

- a. How the hacking of Mr. Azima's computers and emails occurred;
- b. How, when, and by whom Mr. Azima's data came to be published on the BitTorrent websites;

- c. Whether the BitTorrent websites in fact provided public access to Mr. Azima's data;
- d. How, when, and by whom the two websites providing links, and the website concerning Dr. Massaad, were created; and
- e. If possible, to identify the persons who carried out the hacking (or to identify any other circumstances that may be relevant to identifying those persons).

15. In undertaking my analysis and forming the opinions described in this report, I have had access to the following documents and other materials. I describe in more detail below the review of particular materials that I have undertaken:

{F/2/1-12}

- a. SunBlock Systems, Inc., "Azima v. RAK Imaging Summary," November 2, 2016 ("SunBlock Imaging Summary");
- b. A forensic image of Azima's Office iMac, S/N: C02P2DUBF8J2 ("Azima's Office iMac"), that was created in October 2016 by SunBlock Systems, Inc.;
- c. Archived collection of files from an email account (which I understand was used by Azima) fa@fal.us that was collected by BRG on November 18, 2016;
- d. Archived account details of a further Azima email account, fa@farhadazima.com collected by BRG on November 18, 2016;

{F/3/1-13}

- e. SunBlock Systems, Inc., "BitTorrent Download Summary," November 2, 2016 ("SunBlock BitTorrent Summary");
- f. Archive of wetransfer.com file shares collected by BRG on July 13, 2018;
- g. Publicly available documents and websites listed in this report; and
- h. Data files and other materials identified below in this report.

16. I have also been provided with copies of documents produced in this litigation by the parties and the Court, namely:

- {A/1/1-2}** a. The Claim Form and Re-Amended Particulars of Claim;
- b. The Re-Amended Defense;
- c. The Re-Amended Reply;
- {A/6/1-14}** d. Statements providing further information in response to requests (dated
{A/7/1-24} November 2, 2018 and November 6, 2018 served by the Defendant and the Claimant respectively);
- {B/11/1-4}** e. The order of the Court dated October 22, 2018.

17. I have also been provided with a copy of Part 35 of the Civil Procedure Rules, the Civil Justice Council guidance on experts in civil claims, and the model form of expert witness CV published by the Academy of Experts.

18. I refer below to certain documents which I have provided in hard copy in an exhibit submitted with this report (under cover of an index). I have arranged for certain other materials that I have reviewed to be provided in electronic form.

19. BRG Associate Director Ilhwan Yum ("Yum") worked under my direction and supervision to assist me with the investigation and examinations associated with this report. The conclusions I state below are, however, the product of my own expertise and review of the materials.

III. ANALYSIS AND OPINIONS

A. Summary

20. Cyber criminals use fictitiously luring emails, referred to as phishing emails, to gain access without authorization to password protected accounts and computer systems. As

developed below, my analysis indicates that phishing emails were sent to password protected email accounts controlled and used by Azima.

21. It is not remarkable for any email account to receive a certain number of ordinary phishing emails over a period of time. Generic phishing emails can be sent out in large numbers in the same form to many recipients. A specific type of phishing email, however, is in a different category because it involves the recipient being specifically and individually targeted. Where a cyber criminal is seeking to target a particular individual, one methodology is to send phishing emails containing material in the email that concerns or would be of interest to the specific recipient, to further deceive that recipient: these are called 'spear-phishing' emails. Several suspicious emails sent in October and November 2015 included material that related to Azima specifically (or, in one case, an email containing such information was sent to Afsaneh Azadeh, who is described in the Claimant's pleadings as a person acting on Azima's behalf, and who forwarded the email in question to Azima). These constitute spear-phishing emails in the sense I describe. During this time, further phishing emails were also sent to Azima, in addition to the spear-phishing emails.

22. Several of the suspicious emails sent to Azima in this period contained links to external sites, including a link to a site from which a file could be downloaded. In my experience, cyber criminals use phishing emails that (among other things) lure the recipient to open external sites that then have the appearance of a legitimate website and prompt the recipient to enter credentials, or to download files that appear legitimate but which in fact contain malicious software.

23. It is not possible for me to identify the persons who sent any of these spear-phishing emails. This is not surprising, as there are various effective means by which cyber

criminals using the Internet can conceal their identity or location. It is also not possible to say whether my analysis has in fact identified all of the spear-phishing emails that were sent, or indeed detected other methods of gaining unauthorized access. There are several other (often more effective) methods by which unauthorized access can be obtained. Cyber criminal activity is obviously covert. In addition, as I explain below, my analysis does indicate that unauthorized access was gained to Azima's email accounts on multiple occasions in 2015 and 2016. The persons who obtained unauthorized access would have been in a position to delete emails from those accounts (including, in principle, any spear-phishing emails). It is not possible for me to determine whether this occurred, although it is certainly a possibility.

24. Nor can I say which if any of the spear-phishing emails that I have identified ultimately facilitated unauthorized access to Azima's emails and data. This is also not surprising. Considerable time passed between the spear-phishing emails being sent and the time at which Azima appears to have become aware of a possible breach of his Internet security, and my analysis in turn was conducted some time after that; the links in the spear-phishing emails were not able to be fully investigated by the time that my analysis was done.

25. Subject to these points, I am able to say that multiple spear-phishing emails were sent to Azima (including one email sent via Azadeh) in October and November 2015. These were spear-phishing emails because they appear to have contained information about Azima or otherwise targeted at him in some way. At this time also, further phishing emails may have been sent to Azima.

26. My analysis further indicates that at least one of Azima's password protected email accounts was maliciously accessed without Azima's authorization from an online service that promotes itself as providing anonymous Internet traffic that can conceal a user's true identity

and location. Another of Azima's accounts appears to have been accessed in 2015 and/or 2016 from numerous locations, including countries where, as I understand it, Azima had not visited. This evidence suggests that these two accounts were both accessed without authorization, referred to as "hacked."

27. There are networks within the Internet that allow users to share data directly with each other. These decentralized networks make it difficult to identify precise availability and accessibility of the shared data. These networks can allow voluminous amounts of data to be shared, such as the large volume of data stolen from Azima's password protected accounts and devices.

28. Three data files, torrent files, that appeared to contain private data belonging to Azima, were located within the peer-to-peer network BitTorrent in or around August 2016. As described in this report, due to the nature of the BitTorrent network, determining how or by whom these torrent files were published is nearly impossible.

29. While the BitTorrent network requires specialized software to access the network and knowledge of how to navigate the network, the software and network is available to the public.

30. Websites on the World Wide Web are centralized collections of data that users browse to retrieve data. The data can be indexed to make it easier for users to locate specific data. Links to the decentralized network file shares, Azima's stolen data, were placed on indexed webpages, making the stolen data easier to locate. The stolen data was additionally stored in a webserver, allowing Internet users without access to the decentralized file sharing network to easily download the stolen data.

31. Websites providing links to the torrents of Azima's private data were published on or about August 7, 2016 and August 8, 2016. These were web pages on the Blogspot websites, {H10/361/1-2}https://farhadazimascams.blogspot.com (or https://farhadazimascams.blogspot.nl – which routes {H10/360/1-4} to the same web pages), and a website on the Wordpress website, https://exposedfarhadazima.wordpress.com. These websites were published by users "crimeboard," reportedly from "Dubai - United Arab Emirates", and "azamsyed123."

32. The domain www.khater-massaad.com was registered through a privacy service on August 11, 2012. The registrant was then changed on August 13, 2012, to Dimension N Multimedia in Dubai, United Arab Emirates. The registrant was then changed to Ben Anderson on July 29, 2016 and then to a privacy service on November 17, 2016.

33. My examination and investigation of the evidence available to me in this matter did not identify the person or persons who conducted any hacking activities. From my experience in computer hacking cases, cyber criminals take numerous steps to hide their identities and remove traces of their hacking and online activities.

B. Phishing Emails and Account Logins

1. Email Accounts

34. I was provided with a forensic computer image file of the hard drive of an Apple iMac computer, serial number C02P2DUBF8J2 (the "Azima's Office iMac" I mention above). This computer image had a reported MD5 hash value¹ of C2EFB3053AD86DC646A0296E685AF276², which I independently verified.

¹ An MD5 hash is a one-way algorithm that creates a 128-bit value for a computer file, such as the contents of a hard drive. This hash value is like a fingerprint for a file. Any change to the data in the file will change its MD5 hash value.

² SunBlock Imaging Summary. Page 5.

35. During my analysis of Azima's Office iMac, various local copies of the email accounts were located including fa@fa1.us, fa@farhadazima.com, and farhadazima@yahoo.com. These accounts appeared to be used by Azima based on emails sent to and from the accounts.

36. On November 17, 2016, I determined through online research that the email account fa@fa1.us was hosted by GoDaddy's Secure Server Webmail. Through Secure Server Webmail's default settings, the Personal Storage Table ("pst")³ file of emails in the account fa@fa1.us was exported on November 18, 2016. The earliest dated email in this online archive was in March 2016.

37. On November 17, 2016, the activity reports for the account fa@fa1.us was saved by my colleague Yum from the control panel within Secure Server Webmail.

38. On November 18, 2016, Yum determined that fa@farhadazima.com was hosted by Yahoo! Mail. The activity reports for this account was saved from the user interface within Yahoo! Mail.

2. Phishing Attacks

39. Phishing emails ("phishing") are a type of online scam used by criminals to misleadingly evoke an action or response from the user of an email account. Most of the time the online criminals attempt to use a ruse to get the email account user to click on a hyperlink⁴.

40. For example, a cyber criminal will send a fictitious email that appears to come from a reputable company that's commonly used by most consumers. This email may contain

³ A pst file is an email storage file format used to store the contents of an email account, such as messages and calendar events.

⁴ A hyperlink is a connection or reference to a webpage that allows an online computer user to click and go directly to that webpage.

real company logos or brands to make it appear as a legitimate communication from that company. The phishing email will have the user click on a hyperlink or open an attachment that will take the user to a web page the criminal controls.

41. There are many varieties of criminal phishing emails, to include:
 - a. Deceptive phishing is an attack on users where criminals attempt to mimic legitimate companies and entice the user visit a specific web page or to provide personal information or account login credentials to the criminal. The online criminals construct the web page to either look exactly like the real login page or attempt to download malicious software to the user's computer.
 - b. As I explain above, 'spear-phishing' is a more personalized form of phishing. The criminals attempt to make the fraudulent email appear it was personal email by incorporating facts about the intended target.
 - c. Third-party hosted phishing involves criminals abusing online services by hosting web pages within that trusted third-party that tricks the user into believing it is the third-party requesting login credentials. For example, a fraudulent web page hosted within Google Documents can be made to look exactly like an authentic Google login screen. This allows the criminal to have "google.com" as part of the universal resource locator ("URL") of the hyperlink.

3. Phishing Emails

42. As I explain above, it is not uncommon for any email account to receive a quantity of generic deceptive phishing emails. This in itself would not indicate that the individual recipient had been specifically targeted (although together with other facts it may be

relevant to show this). It appears that Azima's email accounts received a quantity of such generic phishing emails over time. Spear-phishing emails are in a different category, however, for two reasons. First, they indicate that the cyber criminal has purposely targeted the deception at that individual (as shown by the fact that the email has been constructed to include material pertinent to the recipient, or otherwise to be of more interest to them). Second, the fact that the spear-phishing email contains material of particular interest to the targeted recipient makes it more likely to be effective, in that the recipient is more likely to open the deceptive email and any further links it may contain.

43. As I explain below, spear-phishing emails were sent to Azima (and Azadeh) in October and November 2015. Moreover, in this time period other phishing emails were also sent to Azima's accounts.

a. October 12, 2015 Phishing Email

{F/4/1-2}

44. On October 12, 2015, email account fa@fa1.us received a forwarded email from "Afsaneh Azedah <Afsaneh@algkc.com>." This forwarded email appeared to have come from "The Huffington Post" but was actually sent to Afsaneh Azadeh from a mesvr.com account, news-reports@huffingtonpost.com.hnfjxqppqogyvxi.mesvr.com.

From: Afsaneh Azadeh <Afsaneh@algkc.com>
Sent: 10/12/2015 2:37:30 PM -0500
To: Farhad Azima <fa@fa1.us>
Subject: Re: Multi-Billionaire Iranian Azima may get in trouble as links against him are getting stronger



Sent from my iPad

On Oct 12, 2015, at 2:29 PM, Farhad Azima <fa@fa1.us> wrote:

I like the Multi-Billionaire part! Where are these Billions?

Sent from my iPad

On Oct 12, 2015, at 8:33 PM, Afsaneh Azadeh <Afsaneh@algkc.com> wrote:

This came to me this morning , in my Alg email account.

Sent from my iPad

Begin forwarded message:

Resent-From: "news-reports@huffingtonpost.com" <news-reports@huffingtonpost.com.huffingtonpost.com>
From: "The Huffington Post" <news-reports@huffingtonpost.com>
Date: October 12, 2015 at 8:19:41 AM CDT
To: afsaneh@algkc.com
Subject: Multi-Billionaire Iranian Azima may get in trouble as links against him are getting stronger
Reply-To: "news-reports@huffingtonpost.com" <news-reports@huffingtonpost.com>

October 9, 2015

THE HUFFINGTON POST

INFORM • INSPIRE • ENTERTAIN • EMPOWER

News

**Multi-Billionaire Iranian Azima
may get in trouble as links
against him are getting
stronger**



By Adam Cooper

Posted: 10/13/2015 09:22 PM EDT | Edited: 10/12/2015 12:12 AM EDT

Reports about the multi-billionaire Farhad Azima are growing as they suggest strong links between Azima and Bin Laden. The source reports point to illegal arms smuggling from a company owned by him in Ghana[[continue reading](#)]

Copyright © 2015 TheHuffingtonPost.com, Inc.
"The Huffington Post" is a registered trademark of TheHuffingtonPost.com, Inc. All rights reserved.

Part of HuffPost Multicultural

Received: (mail 31585 invoked by uid 30207); 12 Oct 2015 19:37:36 -0000
Received: from unknown (HELO p3plbsmtp01-08.prod.phx3.secureserver.net) ([72.167.238.222]) (envelope-sender <atsaneh@alqko.com>) by p3plbsmtp03-03.prod.phx3.secureserver.net (mail-1.03) with SMTP for <fa@fa1.us>; 12 Oct 2015 19:37:36 -0000
Received: from at4mhob14.myregisteredsite.com ([208.17.115.52]) by p3plbsmtp01-08.prod.phx3.secureserver.net with bizzsmtp id UKdc1r00r17sLZD1KdcPA; Mon, 12 Oct 2015 12:37:36 -0700
Received: from mailpod.hostingplatform.com ([10.30.71.203]) by at4mhob14.myregisteredsite.com (8.14.4/8.14.4) with ESMTP id 19CJbYp018542 for <fa@fa1.us>; Mon, 12 Oct 2015 15:37:34 -0400
Received: (mail 11143 invoked by uid 0); 12 Oct 2015 19:37:34 -0000
X-TCPREMOTEIP: 12.130.117.49
X-Authenticated-UID: aa@alqko.com
Received: from unknown (HELO ?172.12.131.160?) (aa@alqko.com@12.130.117.49) by 0 with ESMTP; 12 Oct 2015 19:37:33 -0000
Content-Type: multipart/alternative; boundary=Apple-Mail-D4EFD2FF-B3A8-4689-6829-A24742638837bit
Content-Transfer-Encoding: 7bit
Mime-Version: 1.0 (1.0)
Message-Id: <E83E43A2-82FD-44CF-88FE-1F80CC3F776F@alqko.com>
References: <20181012131942.40A02C56F5@emkai.cz> <79890A86-F16E-4754-828E-D60FA547CA74@alqko.com> <E052F68B-11CC-4CFF-A980-0F14FD7AD1F6@fa1.us> <3052F68B-11CC-4CFF-A980-0F14FD7AD1F6@fa1.us>
In-Reply-To: <3052F68B-11CC-4CFF-A980-0F14FD7AD1F6@fa1.us>
X-Mailer: Pad Mail (13A452)
X-Nonspam: None

45. This email contained a suspicious hyperlink to a website that was not the reported sender of the email nor appeared to be the content provider of the email. This suspicious hyperlink was labeled "continue reading" and had the URL <http://www.nqm6jc1pw57wnk.mesvr.com/tg/nqm6jc1pw57wnlhttp/deferrer.website/kK>. Due to the time between when this email was received into fa@fa1.us and my examination, the functionality of this hyperlink was not able to be investigated as it was when the email was sent on October 12, 2015.

b. October 14, 2015 Phishing Email

46. One possible means by which a specific recipient may be targeted into opening a spear-phishing email is by the email containing information of possible interest to that recipient. From my review of the pleadings, I understand that Azima has interests and business activities involving aviation and airlines.

{F/5.1/1-2} 47. On October 14, 2015, email account fa@fa1.us received an email with the subject "Emirates has shared a video with you on YouTube" sent from "YouTube <alertnotify.564874securitupdat@gmail.com>."

From: YouTube <alerthotly.564574securnupdx@gmail.com>
Sent: 10/14/2015 10:13:57 AM -0700
To: ta@ta1.us
Subject: Emirates has shared a video with you on YouTube



Emirates has shared a video with you on YouTube



Emirates A380 featuring Jennifer Aniston
by Emirates

Our new TV commercial featuring Jennifer Aniston.

Wake up to flying as it should be.

Learn more here: ...

[Help center](#) • [Report spam](#)

©2015 YouTube, LLC 501 Cherry Ave, San Bruno, CA 94066

Received: (qmail 30274 invoked by uid 30297); 14 Oct 2015 17:14:05 -0000
Received: from unknown (msl03-p3plbmt02-05.prod.phx3.secureserver.net [65.178.213.5]) (envelope-sender <alerthotly.564574securnupdx@gmail.com> [alerthotly.564574securnupdx@gmail.com]) by p3plbmt03-04.prod.phx3.secureserver.net (qmail-1.03) with QWTP for <ta@ta1.us>; 14 Oct 2015 17:14:05 -0000
Received: from smtp.mesin.com (51.102.1.54) by p3plbmt02-05.prod.phx3.secureserver.net with bzipmt id VSE31r00; 14 Oct 2015 17:14:05 -0700
Received: from smtp.mesin.com (localhost.localdomain [127.0.0.1]) by smtp.mesin.com (8.14.4.8.13.0/CWT/DCE) with SMTP id SEH0v0014531 (version=TLSv1/SSLv3 cipher=CMR-RSA-AES256-GCM bps=256 verify=NO) for <ta@ta1.us>; Wed, 14 Oct 2015 17:13:57 GMT
Received: (from mail@localhost) by smtp.mesin.com (8.14.4.8.13.0/Submit/CWT/DCE) id SEH0v0014525 for ta@ta1.us; Wed, 14 Oct 2015 17:13:56 GMT
Resent-Date: Wed, 14 Oct 2015 17:13:56 GMT
Resent-Message-Id: <2015101417134525@smtp.mesin.com>
Resent-From: "alerthotly.564574securnupdx@gmail.com"

Received:	<alerntnotfy.564874secuturupdat@gmail.com.ycsethikzpldthv.mesvr.com> from [209.85.213.193] by mesvr.com [91.103.1.64] for <fa@fa1.us> on behalf of alerntnotfy.564874secuturupdat@gmail.com; Wed, 14 Oct 2015 17:13:56 -0700
Received:	from mail-gd4193.google.com (mail-gd4193.google.com [209.85.213.193]) by smtp (8.14.4.8.13.8/CWT/DC2) with SMTP id 156H06YD14479 (version=TLSv1/SSLv3 cipher=RC4- SHA bits=128 verify=OK) for <fa@fa1.us>; Wed, 14 Oct 2015 17:13:55 GMT
Received:	by lgasb17 with SMTP id 4b17605527579gc.1 for <fa@fa1.us>; Wed, 14 Oct 2015 10:13:57 -0700 (PDT)
X-Received:	by 10.50.103.6 with SMTP id b6cme4278104go.26.1444842837655; Wed, 14 Oct 2015 10:13:57 -0700 (PDT)
Received:	by 10.36.37.193 with HTTP; Wed, 14 Oct 2015 10:13:57 -0700 (PDT)
Message-ID:	<CAHLuCOqpl3IECA-cG6H53XU4mqfmlRgubFzgmF8tqjNmXZW@gmail.gmail.com>
Reply-To:	YouTube <alerntnotfy.564874secuturupdat@gmail.com>
MIME-Version:	1.0
Disposition-Notification-To:	"them" <alerntnotfy.564874secuturupdat@gmail.com.ycsethikzpldthv.mesvr.com>
X-Content-Reading-To:	alerntnotfy.564874secuturupdat@gmail.com.ycsethikzpldthv.mesvr.com
Return-Receipt-To:	alerntnotfy.564874secuturupdat@gmail.com.ycsethikzpldthv.mesvr.com
Notice-Requested-Upon-Delivery-To:	alerntnotfy.564874secuturupdat@gmail.com.ycsethikzpldthv.mesvr.com
Errors-To:	alerntnotfy.564874secuturupdat@gmail.com.ycsethikzpldthv.mesvr.com
Content-Type:	text/html; charset=UTF-8
Content-Transfer-Encoding:	quoted-printable
X-Brightmail-Tracker:	H46AAAAAANAAAHgF8AksVR0HGSWpS0cmKPEbnV3z2QAnkvVzdmLUNWV.pRGMD0weLD+1 sAUwRfmsDDVYwZp2W4bZcyW7+SpgJLpDfYcgJREjsV06GqWuRC9wyCusSsc VdEIsTZPaegbHJ3as+4dOYNRQd8ShWYanyao0bV0UdKdSv54QdHE38tngP8aCYEC tMNG08qvCtLreD2SweCqhtAXuInAfS9Qlvmx5CVVY.GAH0Xhzc1a0Z0zH3eQZJwJw Suzp2EMModWYU3F9yQvYISJ2o+AbISGZmGShw6AqoMLJpntTCBnYFQGB8a3OC9Kp GIPQU1U1XVZLSJawC8gr1OFubWvOnFrCyab+Jp8AfPELCOJZZepmWlWAS8yGzps SMScP2akdMOPyWvthvMfY5EORLkQvYGB9Yh1shy4mQvY5H6KkxozPueCvESagU Z0VZ2QD0eakF8hIOHqULUJ5Q2YngWpaaNvF8GdJGS0N6MF8FGCgDdUHL0cpl3uGat tqzH5Jt6Y7Ww2uZ0ZpW6vNSYglzgvfuzpS3MUKASGIGarT04FDC0th9EAU8p Y6qLSAantLUs8M87V4Zp0389qALCtJecub3v0K8gmVPM8DC0uN3S5F1cd8Bdb 3V06g8hM+Zbtp50XOcL8TVU1tdeV7PvH+HxPmISZ3CvFaSE3SPND1qw80nNYP8nK/L MG63FYZXv8PW+2Nc2689v8B5tS0Ux7zvF85vP2dV4Z3ae684mG38VULF8F8yUqJ lba/fmzOcd8b8Y+v42NR8v8tSM5ncVh3XvNZLHMB+HROMDAAA- MSGFPr
X-Homepost:	

48. This email contained suspicious hyperlinks to websites that are not the reported sender of the email, YouTube.com. These suspicious hyperlinks had the domain:

- a. www.5uryv5ovh1asw8.mesvr.com
- b. www.5uryv5ovh1aswk.mesvr.com

Due to the amount of time between when this email was received into fa@fa1.us and my examination, the functionality of these hyperlinks were not able to be investigated as they were when the email was sent on October 14, 2015.

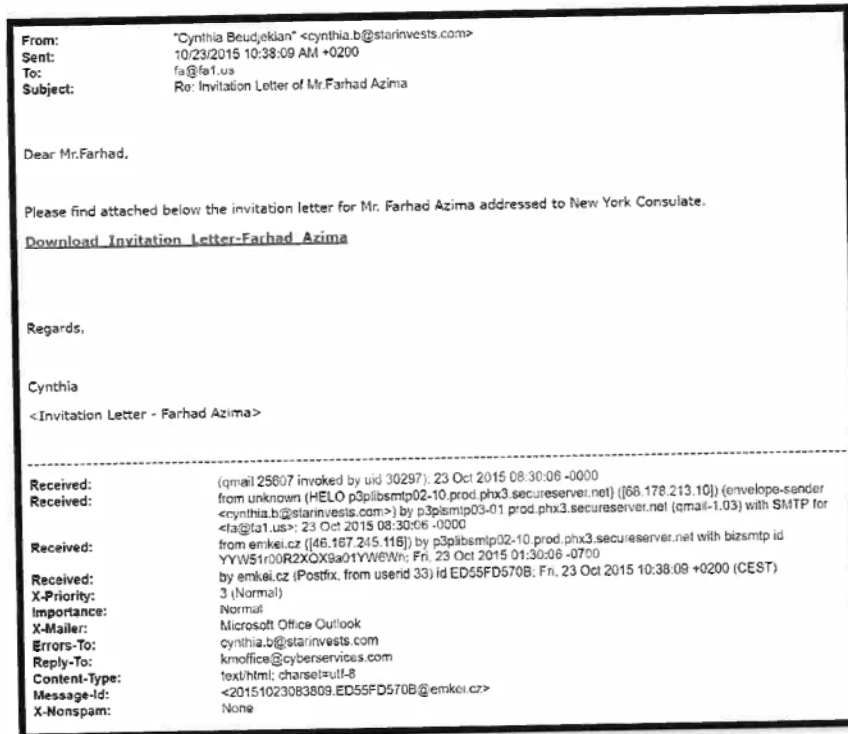
49. Commonly, a YouTube shared video via email lists the sender as "USER NAME⁵ via YouTube <noreply@youtube.com>," not "YouTube <alerntnotfy.564874secuturupdat@gmail.com>," or any variation or having the appearance of a security update title.

⁵ "USER NAME" is generic for any YouTube user name.

c. **October 23, 2015 Phishing Email**

50. On October 23, 2015, email account fa@fa1.us received an email with the subject

{F/5.2/1-1} "Re: Invitation Letter of Mr. Farhad Azima" reportedly sent from "Cynthia Beudjekian <cynthia.b@starinvests.com>."



51. The email header⁶ for the email dated October 23, 2015 contained the settings "Error-To: cynthia.b@starinvests.com" and "Reply-To: kmooffice@cyberservices.com". Replying to this email would address the reply email to kmooffice@cyberservices.com, not the reported sender of the email.

⁶ An email header contains information about the email such as the sender, the receiver, timestamps, and routing information.

{F/5/1-1}

52. The email header for the email dated October 23, 2015 contained information that the email was originally received by "emkei.cz" with the IP address 46.167.245.116. The email header for this email also contained "Message-Id: <20151023083809.ED55FD570B@emkei.cz>." The website emkei.cz is "Emkei's Mailer" and describes it's self as a:

"Free online fake mailer with attachments, encryption, HTML editor and advanced settings...This service does not violate the EU law. We are not obliged to keep any logs. FinalTek.com and Forpsi.com are neither owners nor responsible for its content."⁷

The screenshot shows the Emkei's Mailer website. At the top, there is a "Select Language" dropdown and a Bitcoin logo. The main heading is "Emkei's MAILER" in a stylized, bubbly font. Below the heading, it says "Free online fake mailer with attachments, encryption, HTML editor and advanced settings...". The form includes fields for "From Name:", "From E-mail:", "To:", and "Subject:". There is an "Attachment:" section with a "Choose File" button (showing "No file chosen"), an "Attach another file" button, and an "Advanced Settings" button. The "Content-Type:" section has radio buttons for "text/plain" (selected), "text/html", and "Editor". Below these is a large "Text:" area. At the bottom of the form, it says "Solve reCAPTCHA v2 Instead of v3" and has "Send" and "Clear" buttons. The footer contains copyright information: "© 2009-2019 Emkei • info@emkei.cz" and a disclaimer: "This service does not violate the EU law. We are not obliged to keep any logs. FinalTek.com and Forpsi.com are neither owners of this service nor responsible for its content."

⁷ Emkei's Fake Mailer. Emkei's Mailer. August 28, 2019. <https://emkei.cz/>

53. From my training and experience with cyber hacking, a "free online fake mailer...not obliged to keep any logs" is a tool used by cyber criminals and hackers.

54. The email dated October 23, 2015 contained a suspicious hyperlink to the file sharing website DropBox.com. This suspicious hyperlink was labeled "Download Invitation Letter-Farhad Azima" and had the link https://www.dropbox.com/s/0syupxx3rmjci0j/Invitation_Letter_for_Mr_Farhad_Azima.rar?dl=1. A rar file, as this link was, is a compressed file that holds other files or folders inside.

55. The body of the spear phishing email was addressed to "Mr.Farhad" and contained the message "Please find attached below the invitation letter for Mr. Farhad Azima addressed to New York Consulate." This spear phish was intended to induce "Mr.Farhad" into clicking on what was reported as an invitation letter but was actually a rar file.

56. It was suspicious that an invitation letter would come as a compressed file container of files, a rar file. A downloaded rar file from a spear phishing email was most likely a malicious computer program. Due to the time between when this email was received into fa@fa1.us and my examination, the functionality of this hyperlink and the download of the rar file was not able to be investigated as it was when the email was sent on October 23, 2015.

d. November 23, 2015 Phishing Email

{F/5.3/1-1} 57. On November 23, 2015, email account fa@fa1.us received an email from "Thapanee Chunhachaiphun <thapanee.chunhachaiphun@email.com>." This email appeared to have been sent from "Thapanee Chunhachaiphun" but was actually sent to fa@fa1.us from a mesvr.com account, thapanee.chunhachaiphun@email.com.ypdreqevbyaculk.mesvr.com.

58. This email contained a phishing hyperlink to a website that was not the reported link in the body of the email. This suspicious hyperlink was labeled "https://online.file.transfer/Thapanee_Chunhachaiphun/minutes.of.meeting" but had the URL http://www.g37r3vum5z3wik.mesvr.com/tg/g37r3vum5z3wilhttp/securedownloadfolder.com/Report_on_Minutes_of_meeting_on_financial_support_November_2015_Thapanee_Chunhachaiphun.zip. Due to the time between when this email was received into fa@fal.us and my examination, the functionality of this hyperlink was not able to be investigated as it was when the email was sent on November 23, 2015.

e. November 28, 2015 Phishing Email

{F/6/1-2}

59. On November 28, 2015, email account fa@fal.us received a forwarded email from "Afsaneh Azedah <Afsaneh@algkc.com>." This forwarded email appeared to have come from "Farhad Azima <farhad@farhadazima.com>" but has a "Resent-From" as a mesvr.com account, farhad@farhadazima.com.skqdzpukdevxdk.mesvr.com.

From: Afsaneh Azadeh <aa@algko.com>
Sent: 11/23/2015 3:29:19 AM -0500
To: A <fa@fa1.us>
Subject: Fwd: INV1511648936.PDF

Hi

Everyday I have some strange emails from you . I guess all your emails are infected.

A

Sent from my iPhone

Begin forwarded message:

Resent-From: "farhad@farhadazima.com"
<farhad@farhadazima.com.skcodzoukdevydk.mesvr.com>
From: "Farhad Azima" <farhad@farhadazima.com>
Date: November 28, 2015 at 12:40:17 AM CST
To: afsaneh@algko.com
Subject: INV1511648936.PDF
Reply-To: "farhad@farhadazima.com" <farhad@farhadazima.com>

Farhad Azima has shared the following PDF:
farhad@farhadazima.com

 INV1511648936.PDF

Drive: create, share and store all your stuff in one place.
so15 © Algko.com

Received: (qmail 11212 invoked by uid 30287): 28 Nov 2015 09:29:20 -0000
Received: from unknown (HELO p3plbsmtp01-08.prod.phx3.secureserver.net) (72.167.238.222) (envelope-sender <aa@algko.com>) by p3plbsmtp03-04.prod.phx3.secureserver.net (qmail=1.03) with SMTP for <fa@fa1.us>; 28 Nov 2015 09:29:20 -0000
Received: from at4mhob18.myregisleredsite.com ([209.17.115.111]) by p3plbsmtp01-08.prod.phx3.secureserver.net with b3smtp id mxVK1r00v2C6YGH01xVL3A; Sat, 28 Nov 2015 02:29:20 -0700
Received: from mailpod.hostingplatform.com ([10.30.71.203]) by at4mhob18.myregisleredsite.com (8.14.4/8.14.4) with ESMTP id tAS9THgN040964 for <fa@fa1.us>; Sat, 28 Nov 2015 04:29:17 -0500
Received: (qmail 25376 invoked by uid 0): 28 Nov 2015 09:29:17 -0000
X-TCPREMOTEIP: 76.92.238.175
X-Authenticated-UID: aa@algko.com
Received: from unknown (HELO ?162.168.0.2?) (aa@algko.com@76.92.238.175) by 0 with ESMTPA: 28 Nov 2015 09:29:17 -0000

Content-Type: multipart/alternative; boundary=Apple-Mail-12861D39-294D-485F-A5C4-2AD9264F2185
Content-Transfer-Encoding: 7bit
Mime-Version: 1.0 (1.0)
Message-Id: <1C6F0E34-B48E-473A-8C19-63D5FF282C3B@algko.com>
References: <20151128064017.18928D56A7@emkei.cz>
X-Mailer: iPhone Mail (13B143)
X-Nonspam: None

60. This November 28, 2015 email contained a phishing hyperlink to a website that was not the reported link in the body of the email. This suspicious hyperlink was labeled

"INV1511648936.PDF" and had the URL

<http://www.mo0gpjqisswccck.mesvr.com/tg/mo0gpjqisswccclhttp/deferred.website/43>. Due to the time between when this email was received into fa@fal.us and my examination, the functionality of this hyperlink was not able to be investigated as it was when the email was sent on November 28, 2015.

61. The email header for the email dated November 28, 2015 contained "Reference to <20151128064017.18928D56A7@emkei.cz." This reference, emkei.cz, is the same "free online fake mailer...not obliged to keep any logs" used on the spear phishing email dated October 23, 2015.

f. MESVR

62. The above phishing emails dated October 12, 2015, October 14, 2015, November 23, 2015, and November 28, 2015 were all connected to mesvr.com. All of these phishing emails contained links from mesvr.com and three were sent from mesvr.com.

63. MESVR is a service that can be used by cyber criminals and hackers to obscure the true identity of the email address that sent the email or the phishing links contained in the email. MESVR is sometimes referred to as a wrapper because it "wraps" around a suspicious email address or phishing link to make that email address or link look legitimate. Using an MESVR wrapper to disguise the true identity of the sender by making it look like a legitimate sender is referred to as "spoofing."

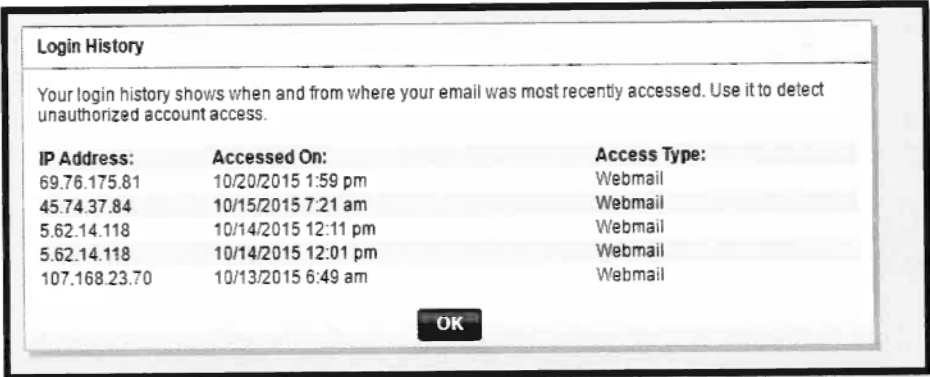
g. Other Phishing Emails

64. My examination of emails was limited to the emails that were stored on Azima's Office iMac when it was forensically imaged by SunBlock Systems on October 16, 2016 and in fa@fal.us when BRG archived the online account on November 18, 2016. I should note the

possibility that Azima's email accounts may have received phishing emails that were not available on that forensic image during my examination.

4. Logins to fa@fa1.us

{F/7/1-1} 65. The login activity report for fa@fa1.us obtained on November 17, 2016 revealed that the user portal of Secure Server Webmail only retains the last five login Internet Protocol ("IP") addresses and timestamps⁸ by default.



Login History		
Your login history shows when and from where your email was most recently accessed. Use it to detect unauthorized account access.		
IP Address:	Accessed On:	Access Type:
69.76.175.81	10/20/2015 1:59 pm	Webmail
45.74.37.84	10/15/2015 7:21 am	Webmail
5.62.14.118	10/14/2015 12:11 pm	Webmail
5.62.14.118	10/14/2015 12:01 pm	Webmail
107.168.23.70	10/13/2015 6:49 am	Webmail

66. The IP addresses 69.76.175.81 that logged into fa@fa1.us on October 20, 2015 was registered to Charter Communications, Inc. Charter Communications reports that IP address was registered in Kansas City, a known location for Azima.

67. The IP address 45.74.37.84 that logged into fa@fa1.us on October 15, 2015 was registered to Internet Security NY.

68. The IP address 5.62.14.118 that logged into fa@fa1.us twice on October 14, 2015 was registered to the virtual private network ("VPN") service provider HideMyAss.

HideMyAss' website describes a VPN as:

VPN stands for Virtual Private Network. It allows you to surf the web anonymously and securely from anywhere. VPNs protect you by creating an

⁸ The default time zone was not available.

encrypted tunnel that connects your computer to the intern, Wi-Fi hotspots and other networks...Switch on your VPN to access the internet. Instead of using your IP address you'll be given on of ours.⁹

69. The IP address 107.168.23.70 that logged into fa@fal.us on October 13, 2015 was registered to Miami Cloud Host.

70. I understand from instructions provided to me by Azima's legal representatives that these IP addresses and registered companies, besides Charter Communications, were unfamiliar to Azima and his associates.

71. My examination of fa@fal.us also revealed emails that containing usernames and passwords for other password protected accounts controlled and used by Azima. Therefore, I believe that the person(s) who had obtained access without authorization to fa@fal.us (and thus to these emails) could have used these details to gain access to other password protected accounts controlled and used by Azima.

5. Logins to fa@farhadazima.com

{F/8/1-1}

72. The authorized connection record and recent access change record for fa@farhadazima.com obtained on November 18, 2016 revealed that Yahoo! Mail provides the user with limited details.

73. The authorized connection record for fa@farhadazima.com listed email access from various countries.

⁹ What is a VPN? HideMyAss. August 5, 2019. <https://www.hidemypass.com/en-us/what-is-vpn>



74. On November 29, 2016, I was informed by Azima's legal representatives that Azima had not been in Bulgaria or India for at least 10 years.

76. On November 29, 2016, I was informed by Azima's legal representatives that Azima had not changed his password more than four times during the last year.

C. BitTorrent

1. The Peer-to-Peer Network

77. Every computer that is online is connected indirectly to every other computer that is online. This indirect connection makes it possible for any two online computers to share information. This is peer-to-peer ("P2P") communication.

78. BitTorrent is a decentralized P2P protocol¹⁰ that can be used to share computer files between online computers.

79. The collection of computers that use the same P2P protocol, such as BitTorrent, are called peers.

80. These peers use a program called a BitTorrent client that allows peers to communicate with other peers.

81. Information about the data file¹¹ that is shared within the BitTorrent protocol is called a torrent file. The torrent file does not contain the shared data but contains information called trackers that allows the client to find the peers that are sharing the data file.

82. The peer that hosts the original data, in its entirety, and that data's torrent file is called a seed. The seed computer then divides the shared data file into many smaller pieces.

¹⁰ A protocol is a defined set of rules that various computers systems agree to use.

¹¹ These data files can be any type of computer files to include a compressed file containing any number of individual files, video files, or image files; any data storage type.

83. A requesting peer uses the client to open a torrent connection for the shared data. The requesting peer will be sent one of the pieces of the shared data and may then get the remaining pieces over time from other peers within the BitTorrent network.

84. Within the BitTorrent network, peers are downloading some pieces of the data file from other peers and uploading additional pieces to different peers. The pieces of the shared data file are spread across many peers, with data duplicated on some peers. The peers that are downloading and uploading pieces of the torrent data are called a swarm. The increased popularity of a torrent will enlarge the number of peers in the swarm.

85. When a peer has finished downloading the torrent data, if that peer is connected to the BitTorrent network, the pieces will continue to be uploaded to other peers in the swarm, called seeding.

86. A peer that has downloaded the entirety of the torrent shared file and allows other peers in the network to download pieces of the shared file are called seeders.

87. If there are any additional seeders for a torrent shared data, the original seed can leave the BitTorrent network with little to no trace.

88. The availability of a shared file may change over time as seeders leave and join the BitTorrent network. It is only possible to download the data from the BitTorrent site when seeders are also on the P2P network.

89. BitTorrent sites have historically been known to share and allow downloads of stolen or pirated data because the BitTorrent network provides some anonymity to the peers.

90. A magnet link contains the information a client needs to a torrent shared data from other peers. The magnet link is a decentralized method that saves the need to download a torrent file to start the shared data download process.

91. Websites can publish magnet links to torrent share files rather than hosting the torrent file on the website.

2. Azima torrent Files

- {F/3/1-13}** 92. I was provided the SunBlock BitTorrent Summary, which summarized as follows:
- a. On October 4, 2016, SunBlock Systems began investigating torrents reportedly related to Azima.
 - b. On October 4, 2016, SunBlock Systems located two torrent shared data, “FARHAD AZIMA OF THE AVIATION LEASING GROUP EXPOSED” (“FarhadExposed”) and “Fraud between Farhad Azima and Jay Solomon” (“Leak Data”), and joined the BitTorrent swarm to attempt to download the data associated with the torrent shares.
 - c. Upon entering the swarm on October 4, 2016, SunBlock Systems did not locate any seeders for FarhadExposed or Leak Data.
 - d. By October 7, 2016, SunBlock Systems was only able to download one piece of the over 3,300 pieces that made up FarhadExposed.
 - e. On October 14, 2016, SunBlock Systems observed a peer in the BitTorrent network with IP address 31.17.249.99 that had joined the swarm. The BitTorrent client indicated that this peer had 24.3% of FarhadExposed.
 - f. That same day, SunBlock Systems observed a peer in the BitTorrent network with IP address 209.133.66.221 that had joined the swarm. The BitTorrent client indicated that this peer had 0.2% of FarhadExposed.

- g. On October 16, 2016, SunBlock Systems observed the same peer with IP address 209.133.66.221 also requested Leak Data. At the time of the observation, this peer had not downloaded any part of Leak Data.
- h. On October 17, 2016, SunBlock Systems observed a peer join the swarm for Leak Data. This peer had the IP address of 223.181.206.95 and had 0.0% of Leak Data downloaded.
- i. On October 21, 2016, SunBlock Systems observed a peer in the BitTorrent swarm with IP address 185.83.180.1. This peer had downloaded 0.4% of FarhadExposed and 0.0% of Leak Data.
- j. SunBlock Systems was able to download 18 pieces of the over 3,300 pieces of FarhadExposed and zero pieces of Leak Data with the seeders available between October 4, 2016 and October 23, 2016.

93. Three torrents that appeared to be connected to Azima were located within the BitTorrent network:

- a. FarhadExposed had a hash value of 1B7E19C3E1406240238169A473B38AFB0C2815D5. This torrent was reportedly 25.75GB in size and appeared to become available on or about August 4, 2016.
- b. Leak Data had a hash value of CA5AF530DCE092A3426EE493A4A5C8409C10B466. This torrent was reportedly 10.33MB in size and appeared to become available on or about August 30, 2016.

- i. This torrent contained 8,063 files, comprised of 7,834 vcard¹² files, 227 Notes files in html format, and two PDF files that contain chat recordings.
 - ii. The PDF files have creation¹³ date attributes around August 29, 2016 at 10:00. The attributes do not include a time zone.
- c. "Farhad Azima's Devices Data Leaked" ("Azima's Devices") had a hash value of 5D65707106C1C7A0562D16f6AE6C90B1AA594B18. This torrent was 4.43GB in size and appeared to become available on September 8, 2016.
- i. This torrent contained 3,497 files, comprised of three text files, 2,550 pictures, 24 videos, 824 audio recordings, and 96 PDF files that contain chat recordings.
 - ii. The PDF files have creation date attributes that range around August 30, 2016 after 6:00 and after 7:00 and August 31, 2016 after 9:00. The attributes do not include a time zone.
 - iii. Of the 2,550 picture files that retained a creation date, the most recent picture was taken on August 24, 2016.

94. Leak'Data and Azima's Devices on were archived by BRG on April 13, 2017.

These torrents were available from seeders with IP addresses 87.236.215.39 (Germany IP

¹² A vCard is a file format standard for electronic business cards.

¹³ Modification, Access, and Creation ("MAC") times are timestamps that are part of a file system's metadata that record defined events that occur to a computer file. These events are described as modification (*i.e.*, when the data in the file is altered), access (*i.e.*, when some part of the file is read), and creation (*i.e.*, when the file was first created). Modification and access times reflect the most recent activity of the file and are overwritten with new events. Once overwritten, prior MAC times are not retrievable.

address that was owned by 1GBits.com and subleased to Cherry Servers, a dedicated server provider) and 151.80.8.16 (France IP address that is owned by OVH and subleased to the Canadian company CheapWindowsVPS.com).

95. As of July 5, 2017, both Leak Data and Azima's Devices were available from the same seeders within the BitTorrent swarm. FarhadExposed remained unavailable.

96. On both July 11, 2017 and August 11, 2017, there were no seeders in the BitTorrent network for any of the three torrents.

3. Tracking Downloads and Availability

97. Obtaining an accurate number of torrent shared file downloads is very difficult, if not impossible, for users of the P2P network.

98. There are a number of tracker sites within the BitTorrent network. While most torrent tracker sites publish "numbers of torrent shared file downloads," these tracker sites do not publish their methodology of calculating the number of downloads.

99. Where a torrent tracker site has no published download counting algorithm, based on my education, training, and experience, I can speculate on two separate possibilities.

- a. Tracker sites are counting how many times their visitors clicked on the listed torrent links, specifically on its site. This will count all attempted downloads, including multiple clicks, regardless of actual completion of file download.
- b. Tracker sites are persistently monitoring torrent swarms to calculate which peers have downloaded a complete set. This will count the existence of users, unique by IP address, with the entire content of the torrent in their possession.

100. As of March 28, 2017, KickAssTorrents¹⁴ reported that the torrent shared file FarhadExposed was downloaded 73 times. For the reasons I give above, it is not possible to say whether any these downloads were actually completed (or if so, how many). Additionally, on that same date, 1337x.to¹⁵ reported that the torrent shared file Leak Data was downloaded 45 times and torrent shared file Azima's Devices was downloaded 63 times. The same qualification applies: it is not possible to say how many times the downloads were actually completed.

101. The published number of torrent downloads also cannot accurately indicate the availability of the torrent without providing dates and times of when the torrents were downloaded (which is information that is not available). For example, all of the reported torrent downloads could have been recorded within the first few days of the torrent link being posted online. Once the seeders went offline, the downloads would have become inaccessible.

D. Data Available on the World Wide Web

1. Websites and Indexing

102. Web browsers are specialized computer software applications that allows users to request data from the World Wide Web, such as web pages. Examples of web browsers are Microsoft's Internet Explorer, Google's Chrome, and Firefox.

103. A website is a group of web pages that contains specialized computer code that defines the format, design, and content of the web pages.

104. Websites are hosted on web servers, specialized online computers that service web browser requests for data, such as web pages.

¹⁴ KickAssTorrents was a website that provided a directory for torrent shared files and magnet links to facilitate P2P file sharing using the BitTorrent protocol.

¹⁵ 1337x.to was a website that provided a directory for torrent shared files and magnet links to facilitate P2P file sharing using the BitTorrent protocol.

105. Web Crawlers are specialized computers that are connected to the World Wide Web and used to systematically go from web page to web page in order to index the content of web pages. The indexing of web pages is the basis of how Internet search engines, such as Google and Bing, allow users to search web pages for specific terms.

2. Data Available on Websites

{H10/361/1-2}
{H10/360/1-4}

106. On December 15, 2016, the websites <https://farhadazimascams.blogspot.nl> ("Blogspot website") and <https://exposedfarhadazima.wordpress.com> ("Wordpress website") were examined and preserved. These websites included magnet links to the torrents such as Leak Data and Azima's Devices. These websites also included labels such as "farhad azima exposed," "farhad azima kansas," and "farhad azima usa."

107. The Blogspot website posts contained a "Last-Modified" data field. This data field appears to be the date and time on the hosting web server when the post was last modified. The "Last-Modified" field does not necessarily correspond to a created or posted date and time, but this timestamp can be used to set a date and time that the post has been available. The oldest post on the Blogpost website is August 7, 2016.

108. The Blogspot website posts were posted by user "crimeboard."

109. The oldest post, August 7, 2016, of user "crimeboard" was tagged with a location of "Dubai – United Arab Emirates."

Sunday, August 7, 2016

Farhad Azima CEO of Aviation Leasing Group - Exposed Again

Farhad Azima was born in 1941. Currently he lives in Kansas City. **Farhad Azima** is chairman for Aviation Leasing Group (ALG).

Farhad Azima found in America's major scandal, the Iran contra affairs and Panama papers. Farhad is Iranian Born and made a career of renting and leasing airplanes. An interesting twist came in his career when he found in the panama papers scandal. "He had no idea about this. He had nothing to do with Panama, said- Farhad Azima." He said that he was investigated by every known agency in United States but they didn't find anything wrong there finally they decided there was absolutely nothing there. It was just a wild goose chase.

But I don't think it was just a wild goose chase because including **Farhad Azima** there are some other personalities who have links to intelligence agencies also found in this scandal. This is his new scam in involvement with some big personality's including his close associates like Ray Adams & Dr. Khater Massaad.

Download

Posted by crimeboard at 10:47 PM

7 comments: Links to this post



Labels: farhad azima exposed, farhad azima fraud, farhad azima kansas, farhad azima scam, farhad azima scammer, farhad azima usa

Location: Dubai - United Arab Emirates

110. The Wordpress website URL naming process includes the upload date into the domain. For example, the link <https://exposedfarhadazima.wordpress.com/2016/08/08/farhad-azimas-devices-data-leaked/> appears to have been created on August 8, 2016. The Wordpress website included URLs starting with:

- <https://exposedfarhadazima.wordpress.com/2016/08/08/>
- <https://exposedfarhadazima.wordpress.com/2016/08/31/>
- <https://exposedfarhadazima.wordpress.com/2016/09/02/>
- <https://exposedfarhadazima.wordpress.com/2016/09/05/>
- <https://exposedfarhadazima.wordpress.com/2016/09/06/>
- <https://exposedfarhadazima.wordpress.com/2016/09/09/>
- <https://exposedfarhadazima.wordpress.com/2016/09/20/>

111. With this URL naming process, the oldest post on the Wordpress website is August 8, 2016.


112. The URL naming convention and timestamps are used in the default page construction for the Wordpress website. There was no evidence found that contradicts that the default naming settings were used for the Wordpress website.

113. The Wordpress website posts were posted by user "azamsyed123."




7/13/2018

First blog about Farhad Azima Scam – Farhad Azima | Farhad Azima Scammer



New York:
New Rule In Minnesota, NY Leaves Drivers Fuming

[Report this ad](#)



New York Drivers With No
Tickets In 3 Years Are In For
A Big Surprise

[Report this ad](#)

[#farhad azima](#) [#farhad azima family](#) [#farhad azima fraud](#) [#farhad azima Iranian Born charter](#) [#farhad azima kansas](#) [#farhad azima scam](#) [#farhad azima usa](#) [#panama papers](#) [#Ray Adams](#)

Published by azamsyed123

Post information about farhad azima [View all posts by azamsyed123](#)

[WordPress.com](#)

<https://exposedfarhadazima.wordpress.com/2016/08/08/farhad-azima-farhad-azima-scammer/>

2/2

3. WeTransfer

114. On July 11, 2018, I was informed by Azima's legal representatives that the websites that had previously hosted torrents and magnet files now allowed the data to be downloaded from directly from websites. Internet users no longer needed the specialized software of BitTorrent or the knowledge of using the P2P network; users could simply click a hyperlink and download the data.

115. On July 13, 2018, I found that the Blogspot posts dated August 7, 2016 and August 11, 2016 had been modified to provided links to the file transfer service wetransfer.com ("WeTransfer"). WeTransfer was being used to host the data, allowing the users of the websites to download the data outside of the P2P network.

116. As of July 13, 2018, all of the ten compressed files (approximately 25GB in total) were accessible. No publicly available evidence was found that indicated if or when any of these files may have been made private or inaccessible since the initial upload.

117. The downloadable content, distributed via WeTransfer, appears to have been at least initially uploaded to WeTransfer on or about January 27, 2017. This date is based on the timestamps and the file identification numbers that are available from the source code of the WeTransfer download webpages. The file identification numbers assigned to the upload appears to contain the date/time and the upload time stamp is accompanied with the size of the upload that matches the data.

4. www.khater-massaad.com

118. Based on publically available domain registration records, the domain www.khater-massaad.com was originally registered through the GoDaddy.com, Inc. privacy service Domains by Proxy, Inc. on August 11, 2011. This registration listed an expiration date of August 11, 2012.

119. On August 13, 2012, two days after the listed expiration date, the registrant was changed to:

Dimension N Multimedia
Unit P12, Rimal, JBR
Dubai, Dubai 487177
United Arab Emirates
Administrative and technical contact was Alain Morcos

120. On July 29, 2016, the domain was registered through the registrar Ascio Technologies, Inc. in Denmark and the registrant was listed as:

Ben Anderson
NetNames Ltd.¹⁶
3rd Floor Prospero House
241 Borough High St.
London, GB
SE1 1GA

121. On November 17, 2016, the publically listed registrant was changed to Domain Trustees UK Limited, a Ascio Technologies, Inc. privacy service.

E. Summary of Conclusions

122. Cyber criminals sent numerous spear-phishing emails to Azima in October and November 2015, containing deceptive links. Spear-phishing is a common means of gaining access to password protected accounts and computer systems. At least one of Azima's accounts was maliciously accessed in October 2015 from IP addresses unfamiliar to Azima, including using the online service HideMyAss in order to disguise the user true IP address. Another email account appears to have been accessed from numerous locations around the world including locations where Azima was not present. The email accounts also in turn contained the details (including login credentials) for other email addresses used by Azima.

123. In my opinion, the security of Azima's email accounts were compromised and it would therefore have been possible for the persons gaining unauthorized access to obtain access to and to download data accessible through those accounts. My analysis has not ascertained whether further breaches occurred by other means, or whether unauthorized access was obtained

¹⁶ NetNames Ltd. provides online brand protection, domain name management, and domain name acquisition services.

to any of Azima's computers (as opposed to his email accounts, and data accessible through those accounts including through cloud storage).

124. The P2P networks, in this case BitTorrent, allow users to share stolen data directly with each other, which makes it difficult to identify when the stolen data was available and how accessible the stolen data really was to a third party. The BitTorrent network allowed cyber criminals to share a large volume of data stolen from Azima's password protected accounts and devices. It is not clear whether or to what extent those BitTorrent sites did in fact facilitate the sharing and dissemination of Azima's data. The analysis I have reviewed indicates that it was not possible for SunBlock to download the data set in October 2016. My analysis indicates moreover that access to the data through ordinary Internet sites (ie, the WeTransfer sites, which are not peer-to-peer or torrent sites) was subsequently established, in January 2017.

125. Setting up websites on the World Wide Web with links to Azima's stolen data allowed the web pages to be indexed, make it easier for users to locate the specific data. The two websites (the Blogspot and the Wordpress websites) providing links to the sites hosting Azima's data were such websites. It is difficult to identify the persons responsible for those sites; one person placing posts on one of the sites was, however, reported as being based in Dubai in the United Arab Emirates. Further, putting the stolen data on a web-based file share allowed Internet users without access to BitTorrent to easily find and download the stolen data.

DECLARATION STATEMENTS

126. I understand, have complied with, and will continue to comply with my duty to the court.

127. I am aware of the requirements of CPR 35, PD 35 the Guidance and the Pre-action Practice Direction.

128. I confirm that I have made clear which facts and matters referred to in this report are within my own knowledge and which are not. Those that are within my own knowledge I confirm to be true. The opinions I have expressed represent my true and complete professional opinions on the matters to which they refer.



August 30, 2019

Christopher W. Tarbell